Section IV: **Network Security**
Title: **Telecommunication Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **May 7, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To safeguard the protected information that is communicated over the North Carolina (NC) Department of Health and Human Services (DHHS) telecommunication network.

STANDARD

1.0 Background

The DHHS workforce relies daily on the DHHS telecommunication network to complete their work efficiently. Some DHHS workforce members use the DHHS telecommunication equipment to communicate confidential information to outside entities. When this occurs, the Divisions and Offices shall ensure that adequate procedures are established and monitored to effectively protect information as it traverses the public telecommunication network.

There are three (3) categories of telecommunication that are covered within this standard:

- Public electronic communication is any element of data that is transmitted or received via a public telecommunication network. This *digital* mode of communication includes, but is not limited to the following:
  - Public Switch Telephone Network (PSTN)
  - Fiber Optics
  - Coaxial Cable
- Public image communication is any element of an image that is transmitted or received via a public telecommunication network. This *image* mode of communication includes, but is not limited to the following:
  - Electronic fax
  - Paper fax
- Public verbal communication is any element of a voice that is transmitted or received via a public telecommunication network. This *verbal* mode of communication includes, but is not limited to the following:
  - Plain Old Telephone Service (POTS)
  - Private Branch Exchange (PBX)
  - Voice over Internet Protocol (VoIP)
  - Cellular Phone Service

Public telecommunication network technologies include but are not limited to the following:

- Coaxial Cable
- Cellular Radio Network (CRN)
- Digital Subscriber Line (DSL)
- Ethernet
- Fiber Optics
- Integrated Services Digital Network (ISDN)
- Voiceband Modem
- Voice over Internet Protocol (VoIP)

2.0 Confidentiality

The Division or Office shall ensure that confidential information is safeguarded in the following manner:

- If a Division carries out *public electronic communication* with any outside entity or between offices and any part traverses a public telecommunication network, then the Division Information Security Official (ISO) shall ensure that the following are documented, monitored, and verified:
  - Points of ingression and egression, executed as defined in the NC DHHS Security Standards, Network Security Standards – Remote Access and Virtual Private Networks (VPNs) Security Standard
  - Publish a procedure for their workforce members to ensure this information has been approved for disclosure
- If a Division carries out *public image communication* with any outside entity or between offices and any part traverses a public telecommunication network, then the Division ISO shall perform the following:
  - Publish a procedure for their workforce members to ensure this information has been approved for disclosure
  - Publish a procedure for their workforce members to ensure that proper authentication is carried out prior to communicating this information
- If a Division carries out *public verbal communication* with any outside entity or between offices and any part traverses a public telecommunication network, then the Division ISO shall perform the following:
  - Publish a procedure for their workforce members to ensure this information has been approved for disclosure
  - Publish a procedure for their workforce members to ensure that proper authentication is carried out prior to communicating this information

3.0 Documentation

The Division ISO shall maintain current telecommunication configuration records on all telephone systems, including but not limited to the following: outside wiring, inside wiring, cabling, telecommunication devices, wiring closets, telecommunication equipment, etc. All telecommunication devices connected to the DHHS telecommunication network must be registered and approved by the Division ISO prior to being installed. The Division ISO shall strictly control access to the telecommunication configuration records. Prior to being released, all requests for telecommunication records must be submitted to and approved by the Division ISO in writing to avoid any type of tampering or malice.

If unauthorized activity is suspected or detected, every effort shall be made to immediately isolate the telecommunication device in question and trace it to a physical location. All unauthorized activities shall be immediately reported as an incident in accordance with the NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual, Information Incident Management Policy.

References:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 3 – Processing Information and Documents, Section 04: Telephones and Fax
    - Standard 030401 – Making Conference Calls
    - Standard 030402 – Using Videoconferencing Facilities
    - Standard 030403 – Recording of Telephone Conversations
    - Standard 030404 – Receiving Misdirected Information by Facsimile
    - Standard 030405 – Giving Information When Ordering Goods on Telephone
    - Standard 030406 – Persons Giving Instructions Over the Telephone
    - Standard 030407 – Persons Requesting Information Over the Telephone
    - Standard 030408 – Receiving Unsolicited Facsimiles

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Classification Security Standard
    - Network Architecture Security Standard
    - Network Security Standards
    - Personnel Issues Related to Information Security Standard
    - Remote Access and VPNs Security Standard
    - Wireless Security Standards

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Information Incident Management Policy
  - Network and Telecommunication Security Policy